What is claimed is:

1. A method comprising:

performing an authentication of a computing device and equipment of an operator of services for the computing device for a session of communication between the computing device and the equipment, the performing comprising:

generating, in the computing device, a random number;

generating a one-time-pad key based on a hash operation of a value selected from the group consisting of an identification of the computing device, an identification of the equipment, a platform configuration measurement of the computing device stored in a protected storage within the computing device and an identification of the session of communication stored in the protected storage within the computing device;

encrypting the random number based on the one-time-pad key;

transmitting the encrypted random number to the equipment;

receiving, from the equipment, an encrypted value in response to the encrypted random number, wherein the encrypted value includes a challenge of a challenge-response;

verifying the encrypted value;

encrypting a response to the challenge of the challenge-response;

transmitting the response to the equipment; and

receiving, from the equipment, an authentication verification.

2. The method of claim 1, wherein the platform configuration measurement of the computing device comprises a version of hardware in the computing device.

3. The method of claim 1, wherein the platform configuration measurement of the computing device comprises a version of software executing in the computing device.

4. The method of claim 1, wherein the challenge of the challenge-response comprises an encryption of a data string that includes a concatenation of the random number generated in the computing device, a random number generated by the equipment and the identification of the session.

5. The method of claim 4, wherein the response of the challenge-response comprises an encryption of a data string that includes a concatenation of the random number generated in the computing device and the random number generated by the equipment.

6. The method of claim 1, further comprising auditing the authentication, wherein auditing comprises:

storing at least one attribute of the authentication into an audit log within a memory of the computing device;

encrypting the audit log based on an encryption key that is generated and stored within the computing device;

generating an integrity metric of the audit log; and

generating a signature of the integrity metric with a signature key that is generated and stored within the computing device.

7. The method of claim 6, wherein auditing the authentication further comprises generating a signature of a value of an audit counter with the signature key.

8. A method comprising:

authenticating a computing device and a different entity for a session of communication between the computing device and the different entity, the authenticating comprising:

generating a hash of a value selected from the group consisting of a platform configuration value associated with computing device stored in the

computing device and the identification of the session stored in a protected storage within the computing device and;

encrypting a random number based on the hash; and

transmitting the encrypted random number to the different entity.

9. The method of claim 8, wherein the authenticating further comprises:

encrypting a response to a challenge of a challenge-response, wherein the challenge is received, in response to the encrypted random number, as part of an encrypted value from the different entity; and

transmitting the encrypted response to the different entity.

10. The method of claim 8, further comprising commencing a transaction between the computing device and the different entity, after receiving an authentication verification message in response to the encrypted response from the different entity.

11. The method of claim 8, further comprising auditing the authenticating, wherein auditing comprises:

storing at least one attribute of the authenticating into an audit log within a memory of the computing device;

encrypting the audit log based on an encryption key that is generated and stored within the computing device;

generating an integrity metric of the audit log; and

generating a signature of the integrity metric with a signature key that is generated and stored within the computing device.

12. The method of claim 11, wherein auditing the authenticating further comprises generating a signature of a value of an audit counter with the signature key.

13. The method of claim 12, wherein auditing the authenticating further comprises appending the integrity metric, the signature of the integrity metric, the signature of the value of the audit counter and the value of the audit counter to the audit log.

14. The method of claim 8, wherein the platform configuration value associated with the computing device comprises a version of hardware in the computing device.

15. The method of claim 8, wherein the platform configuration value associated with the computing device comprises a version of software executing in the computing device.

16. A method comprising:

authenticating a computing device and equipment of a provider of services for the computing device for a session of communication between the computing device and the equipment, the authenticating comprising:

receiving a number that is encrypted with a hash of a value selected from the group consisting of a platform configuration value associated with computing device stored in the computing device and the identification of the session;

recovering the number; and

encrypting, in response to receiving the hash, a value from the group consisting of a challenge of a challenge-response that includes the number, a random number generated in the equipment and an attestation key; and

transmitting the encrypted value to the computing device.

17. The method of claim 16, wherein authenticating further comprises generating the challenge of the challenge-response, wherein generating of the challenge comprises encrypting, using the session key, from values selected from

the group consisting of the number from the computing device, the random number generated in the equipment and a different identification of the session.

18. The method of claim 16, wherein authenticating further comprises:

receiving a response of the challenge-response, wherein the response is encrypted;

decrypting the response that is encrypted; and

verifying that the response includes values selected from the group consisting of the number from the computing device and the random number generated in the equipment.

19. The method of claim 16, wherein the platform configuration value associated with the computing device comprises a version of hardware in the computing device.

20. The method of claim 16, wherein the platform configuration value associated with the computing device comprises a version of software executing in the computing device.

21. A system comprising:

a Synchronous RAM (SRAM) to store at least a part of a number of instructions to cause authentication of the system to equipment of a provider of services for the system and to cause authentication of the equipment to the system;

a processor to execute the number of instructions;

a cryptographic processing module comprising:

at least one storage register to store an encrypted configuration associated with the system and an identification of a session of communication between the system and the equipment of the provider of services for the system;

a random number generation logic to generate a random number;

a hashing logic to generate, based on the execution of the number of instructions, a hash of a value selected from the group consisting of the encrypted

configuration associated with the system and the identification of the session of communication; and

an encryption logic to encrypt the random number based on hash;

an input/output (I/O) logic to transmit the random number to the equipment of the provider of services for the system.

22. The system of claim 21, wherein the I/O logic is to receive an encrypted message from the equipment, in response to the random number, wherein the encrypted message includes values from the group consisting of a challenge of a challenge-response, a random number generated in the equipment and an attestation key.

23. The system of claim 21, wherein the encryption logic is to encrypt a response to the challenge of the challenge-response, wherein the I/O logic is to transmit the encrypted response to the equipment of the provider of services for the system.

24. The system of claim 23, wherein the I/O logic is to transmit a communication with an entity on a network to which the equipment is coupled after receipt of an authentication message from the equipment in response to the encrypted response.

25. A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

performing an authentication of a computing device and equipment of an operator of services for the computing device for a session of communication between the computing device and the equipment, the performing comprising:

generating, in the computing device, a random number;

generating a one-time-pad key based on a hash operation of a value selected from the group consisting of an identification of the computing device, an

identification of the equipment, a platform configuration measurement of the computing device stored in a protected storage within the computing device and an identification of the session of communication stored in the protected storage within the computing device;

encrypting the random number based on the one-time-pad key;

transmitting the encrypted random number to the equipment;

receiving, from the equipment, an encrypted value in response to the encrypted random number, wherein the encrypted value includes a challenge of a challenge-response;

verifying the encrypted value;

encrypting a response to the challenge of the challenge-response;

transmitting the response to the equipment; and

receiving, from the equipment, an authentication verification.

26. The machine-readable medium of claim 25, wherein the challenge of the challenge-response comprises an encryption of a data string that includes a concatenation of the random number generated in the computing device, a random number generated by the equipment and the identification of the session.

27. The machine-readable medium of claim 26, wherein the response of the challenge-response comprises an encryption of a data string that includes a concatenation of the random number generated in the computing device and the random number generated by the equipment.

28. A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

authenticating a computing device and a different entity for a session of communication between the computing device and the different entity, the authenticating comprising:

generating a hash of a value selected from the group consisting of a platform configuration value associated with computing device stored in the

computing device and the identification of the session stored in a protected storage within the computing device;

encrypting a random number based on the hash; and

transmitting the encrypted random number to the different entity.

29. The machine-readable medium of claim 28, wherein the authenticating further comprises:

encrypting a response to a challenge of a challenge-response, wherein the challenge is received, in response to the encrypted random number, as part of an encrypted value from the different entity; and

transmitting the encrypted response to the different entity.

30. The machine-readable medium of claim 28, further comprising commencing a transaction between the computing device and the different entity, after receiving an authentication verification message in response to the encrypted response from the different entity.

31. A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

authenticating a computing device and equipment of a provider of services for the computing device for a session of communication between the computing device and the equipment, the authenticating comprising:

receiving a number that is encrypted with a hash of a value selected from the group consisting of a platform configuration value associated with computing device stored in the computing device and the identification of the session;

recovering the number;

encrypting, in response to receiving the hash, a value from the group consisting of a challenge of a challenge-response that includes the number, a random number generated in the equipment and an attestation key; and

transmitting the encrypted value to the computing device.

32. The machine-readable medium of claim 31, wherein authenticating further comprises generating the challenge of the challenge-response, wherein generating of the challenge comprises encrypting, using the session key, from values selected from the group consisting of the number from the computing device, the random number generated in the equipment and a different identification of the session.

33. The machine-readable medium of claim 31, wherein authenticating further comprises:

receiving a response of the challenge-response, wherein the response is encrypted;

decrypting the response that is encrypted; and

verifying that the response includes values selected from the group consisting of the number from the computing device and the random number generated in the equipment.